

SCR Initiatives

Comparative Information for NIST SwAF



digital

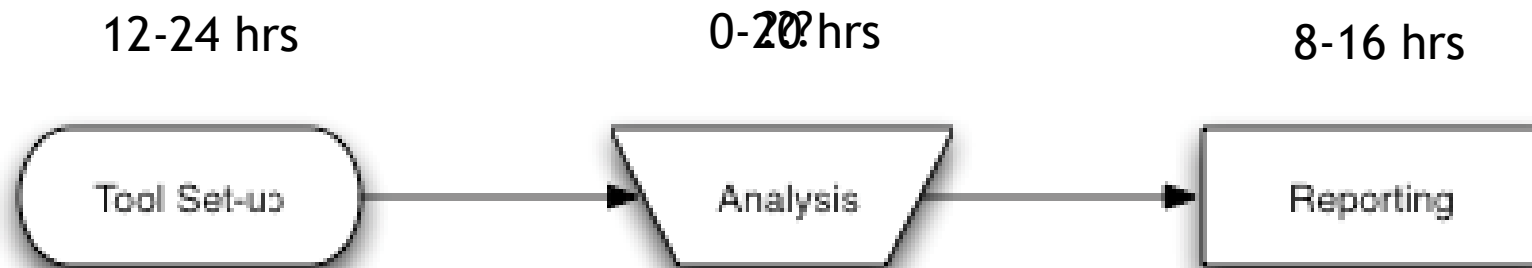
Software Confidence. Achieved.

John Steven
Senior Director

jsteven@digital.com

703.727.4034

State of the Practice - Code Assessments



- ◆ It takes a day and a half to get results
- ◆ It takes a day or two to report
- ◆ That leaves very little time for thinking

State of Demand: SCR Volume

◆ Central

- 13.5 MLoC
- 200 Apps / yr.
- 50 MLoC
- 100 MLoC

◆ Self Service (per year)

- 550 Apps (23MLoC)
- 300 Apps (35 MLoC)
- 350 Apps (14 MLoC)

◆ Aspirations

- 100+ MLoC / day
- 1000s Apps / yr



Selecting Applications

- ◆ BSIMM: 'no org' does portfolio risk rating
- ◆ Risk models in place pick:
 - Automated vs. Manual approach
 - Tools (Veracode, AppScan Source, Fortify, Findbugs, CAT.NET, etc.)
 - LoE for manual efforts, results triage
- ◆ Orgs picking from *internal* + external apps



Outstanding Issues

- ◆ Several arguments persist:
 - Where do SCR tools fit?
 - Who pays for this? (Audit, Security, Business)?
 - Can SCR be combined with other assurance methods?
 - Where can this work be done?
 - What skill-set is necessary to complete this work?



Tool Gaps

- ◆ Submission portal (3)
- ◆ Reporting Tool (2)
- ◆ Assembly Line (4)
- ◆ Enterprise Reporting



Staffing Trends

- ◆ Triage
 - 2-5 persons
 - Tool vendor management
- ◆ Review
 - 0-24 reviewers
 - Some organizations remain entirely domestic
- ◆ Use vendors
 - Spike management
 - On-boarding

Emerging Roles

- ◆ On-boarding specialist
 - *Highly technical & experienced*
 - Writes custom rules for org. in self-service
- ◆ Security Researcher
 - Interfaces with tool vendor
 - Extends scanning capabilities
- ◆ QA
 - Conducts results triage



Costs

◆ Licensing

◆ Staff

- \$820K

- \$5MM

◆ Total Cost: (Licensing, Staff, Services)

- \$4.8MM

- \$9.2MM



Doing the work

◆ Perform scan & generate a results file

- 2 calendar days, 16 mhrs
- 7 calendar days, 24-32 mhrs
- 14 calendar days, 40 mhrs

◆ Conduct Review:

- 0 mhrs
- 1-2 calendar weeks, 20-50 mhrs
- 2-4 calendar weeks, 80-160 mhrs



How to Close the Gaps

What organizations are addressing



digital

Software Confidence. Achieved.

Goals

- ◆ Reduce total cost of application assessment by:
 - Increasing automation of menial tasks
 - ‘Remembering’ previous assessment configuration/information
 - Raising *inter-reviewer* consistency
- ◆ Increase depth by:
 - Highlighting security-relevant implementation/design
 - Conducting meaningful analysis current tools can’t
 - Supporting rapid prototyping of truly advanced capabilities

“Focus reviewers on code-understanding, and meld them with the tool, leveraging the strengths of both”



Solution Topology

What organizations are addressing



digital

Software Confidence. Achieved.

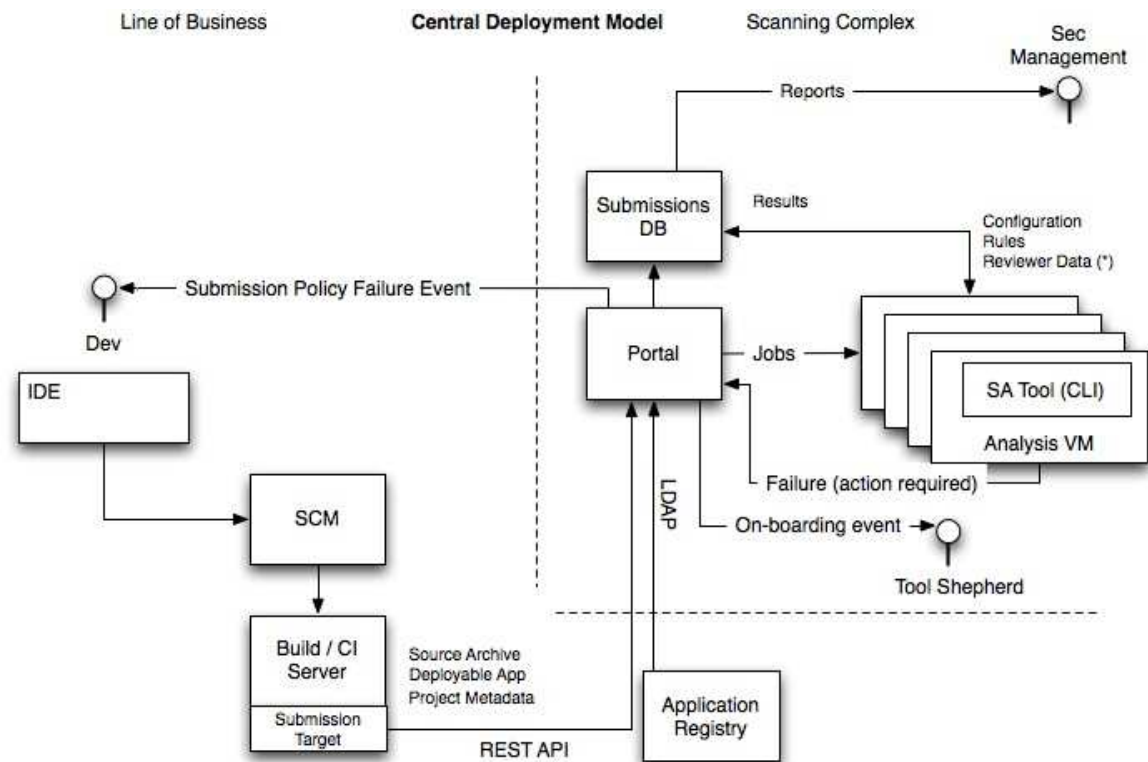
Integration Submission - Push

◆ Integrate with LoB

- Place shim in build/CI/QA environment
- Archive
 - ◆ source,
 - ◆ deployable binary
 - ◆ project meta
 - ◆ SCR meta
- Submits using REST

◆ Portal

- Save
 - ◆ Configuration
 - ◆ Rules
 - ◆ Reviewer data
 - ◆ Results



Integration Results

◆ Reviewer

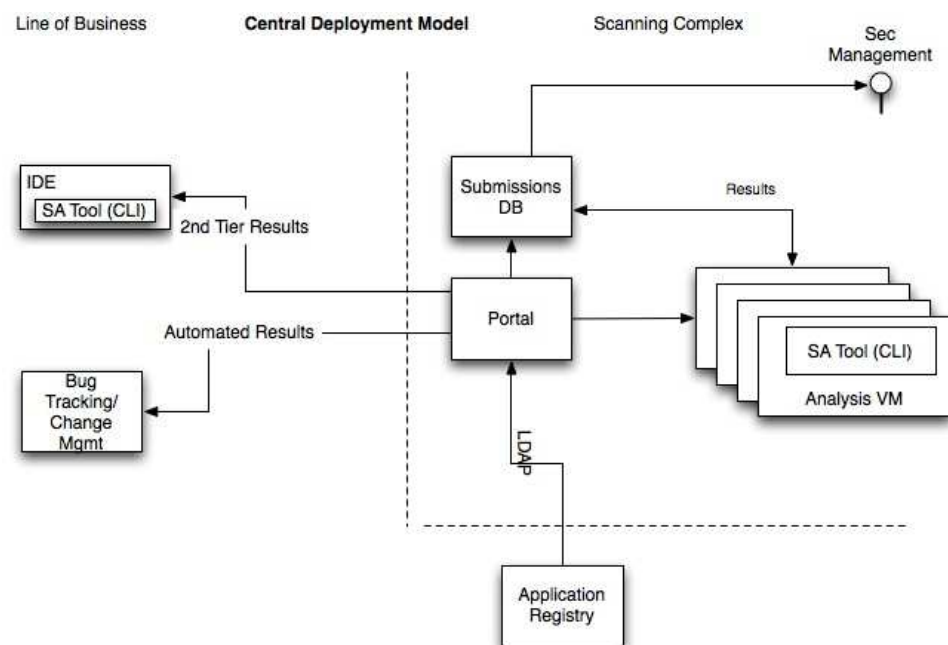
- Notified of need to update SCR config
- Escalated SCRs

◆ Developer

- Receives automated results from bug tracking
- Receives 2nd tier of results in plug-in
- Later, will receive custom desktop-based rules based on results

◆ QA

- Triage 2nd tier results, makes assignments



Rules Management

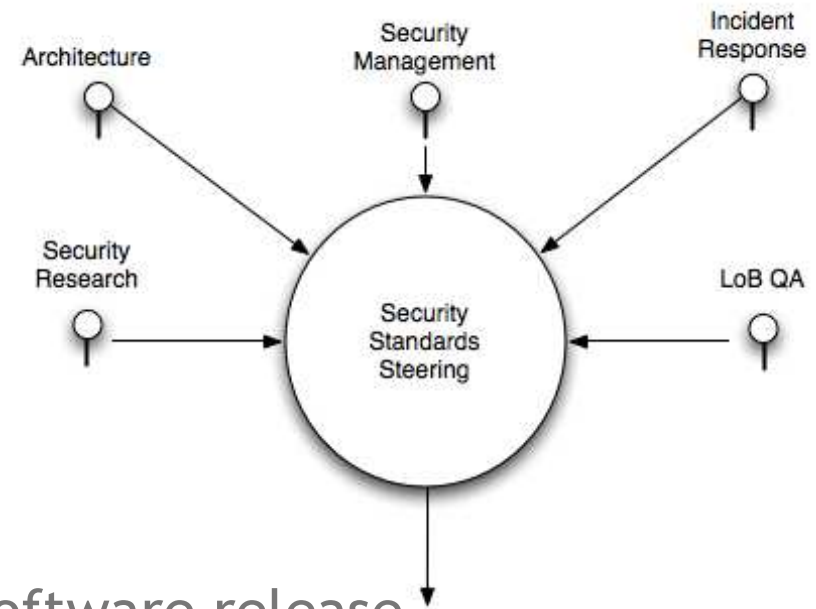
What organizations are addressing



digital

Software Confidence. Achieved.

Source of Rules



◆ Manage rules conceptually

- Treat rules, tool config. as software release (testing, versioning)
- Select optimal assurance tool for rule
- Combine proactive & reactive rule sources
- Acknowledge multiple stakeholders

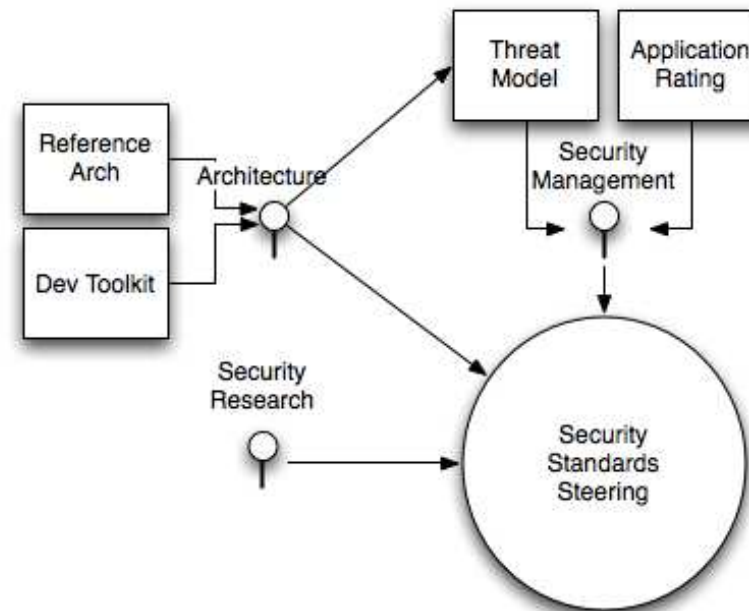
◆ Deploy rules automatically

Proactive Stakeholders

◆ Threat Model/App Rating

- Drive assessment type, frequency
- Generate configuration
- Drive # of rules
- Drive rules for attack surface

◆ Maturity of app possible



Reactive Stakeholders

◆ Actual Incidents

- Drive high priority
- Generate new rules

◆ Assessment Data

- Drives rules priorities
- Drives reduction of false positives
- Creates application-specific rules
- Creates framework-specific rules

